Observe PCI DSS:
How to Audit Application Activity When Logs Don't Help

Extended Version

Dr. Anton Chuvakin

SecurityWarrior LLC http://www.securitywarriorconsulting.com

anton@chuvakin.org

(510) 771-7106

Executive Summary

This paper covers the critical challenges of implementing PCI DSS controls and suggests creative solutions for related compliance and security issues. Specifically, the hard problem of security monitoring and log review in cloud, legacy, and custom application environment is discussed in depth. Additionally, clarification of key PCI DSS compensating controls is provided. This paper will help you satisfy the regulatory requirements and improve security of your sensitive and regulated data.

Introduction

If you are like most information technology (IT) professionals, the idea of becoming compliant with PCI DSS or countless other regulations does not sound like an enjoyable task. However, implementing security controls and practices in order to be compliant with PCI DSS or other regulations is a daily reality at thousands of organizations today. In addition, information security and regulatory compliance are related in the minds of many executives as well as IT professionals.

This paper will review some of the challenges in implementing PCI DSS controls and suggest some of the creative solutions for compliance and security problems.

PCI DSS Revealed

Visa, MasterCard, American Express, Discover, and JCB banded together to develop PCI DSS to ensure that credit card customer information is adequately protected - and to protect the payment card industry itself. As more and more purchases and transactions are done with credit and debit cards, the importance of protecting cardholder information as well as electronic transaction integrity can only grow. Visa alone does $5.2 trillion dollars in payment card transaction every year, which exceeds the individual GDP volumes of all but four countries on the planet.

The Payment Card Industry Data Security Standard (PCI DSS) applies to organizations that either accept payment cards or handle payment card data. PCI Council, charged with maintaining the standards since 2004, states that "the PCI DSS applies to any entity that stores, processes, and/or transmits cardholder data" (https://www.pcisecuritystandards.org/pdfs/pcissc_overview.pdf). This broad applicability statement makes PCI one of the most influential security regulations today. What adds to the power of PCI DSS is a power of compliance enforcement, wielded by the global card brands.

As a result, millions of businesses worldwide have to validate and then maintain PCI compliance. From small stores to giant hotel chains to global airlines, PCI DSS makes its mark on how organizations implement information security controls. In fact, PCI's impact has grown beyond its original mission of protecting confidentiality of card data and reducing risk of card transactions, and now has started to serve as a foundation for security programs at many organizations.

Despite a number of myths about PCI DSS applicability, PCI DSS does apply to every organization that accepts payment cards. To better understand PCI, it is useful to separate the PCI regulatory regime, covering the compliance enforcement via fines and on-site assessments, from the PCI DSS guidance document itself. Organizations subject to PCI DSS are subject to either annual on-site assessment, performed by a Council-certified assessor - QSA, or an annual self-assessment. Maintaining the compliant status between assessments is mandatory and falls under the responsibility of the organization. In case of a card data breach, such compliance status will definitely be rechecked as has happened after recent mega-breaches. The entire PCI

DSS document contains slightly over 220 security controls covering both technical and policy controls, and ranging from vulnerability scanning, through log review and to security awareness training and incident response planning.

But despite its success over the last few years, PCI has occasionally influenced security thinking in less useful ways. Some businesses choose to treat PCI DSS as "ceiling, not a floor, of security" and blindly implement only PCI controls while neglecting all others. Also, other types of data that businesses use deserve no less protection than payment data. Organizations should not lose focus on other types of secret and sensitive data, both internal and regulated, especially when its loss can be even more damaging than payment data.

Today, after a few revisions, PCI DSS stands at version 2.0, which will continue to be the active version for the next 3 years. In brief, PCI DSS's 12 broad requirements are:

PCI Data Security Standard – High Level Overview

Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need to know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes.
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for all personnel.

(Source: PCI Council website https://www.pcisecuritystandards.org, PCI DSS v2.0 document)

PCI compliance presents a significant challenge to large, distributed businesses. While getting compliant is easier than staying in compliance, even that initial assessment often takes months of work and thousands of dollars in products and services, as well as internal policy changes. Legacy applications as well as newer virtual and even cloud based applications, falling under PCI mandate, present additional challenges.

On the other end of the spectrum, smaller, less security aware organizations face their own dramatic PCI challenges, related to costly ongoing controls, such as log monitoring, as well as controls requiring extensive security knowledge, such as secure application development. Even with simpler security controls such as avoiding default passwords and configuring firewalls, smaller organizations have trouble protecting their data. The recent Verizon Data Breach Investigations 2011 report, for example, still names password guessing as a key risk to card data: '"exploitation of default or guessable credentials" is represented in two-thirds of all intrusions and accounts for nearly one-third of all [sensitive data] records compromised.'

In practice, none of the breached organizations to date has been found to be compliant at the time of the breach. Many controls were missing or implemented incorrectly, which lead to a breach. Some of the recent cardholder data breaches include TJX retail stores, Heartland processor and many smaller businesses worldwide. Industry research suggests that properly implementing PCI controls leads to reduced chances of becoming a breach victim.

Compensating Controls in PCI DSS

As we mention above, PCI mandates the implementation of hundreds of controls, often in a clearly prescriptive manner. What happens if an organization is unable to implement security in exactly the manner mandated by the DSS standard? The key concept here is "compensating control" which is defined in the standard as follows: *"Compensating controls may be considered for most PCI DSS requirements when an entity cannot meet a requirement explicitly as stated, due to legitimate technical or documented business constraints." Such controls must "Meet the intent and rigor of the original PCI DSS requirement" while "Being "above and beyond" other PCI DSS requirements."*

This simply means that organizations must implement another security measure, which is as good as or better than the PCI prescribed control. In case of on-site assessments, the QSA will usually approve the controls that follow the spirit and intent of the original requirement. Quoting from the "PCI Compliance" book by the author, "*Compensating controls are challenging. They often require a risk-based approach that can vary greatly from one Qualified Security Assessor (QSA) to another. There is no guarantee a compensating control that works today will work one year from now, and the evolution of the standard itself could render a previous control invalid.*"

In some cases, the use of compensating controls is not only permissible, but unavoidable. For example, consider a legacy payment application that does not have the logging features, covered in PCI DSS Requirement 10, such as relating all actions to users and logging the necessary details. Sometimes, the application cannot be replaced for legitimate business reasons. Despite such application limitations, the organization still needs to become and stay compliant - and the only way to do it is through the use of compensating controls.

Here are some of the examples of PCI requirements that commonly use compensating controls (from the same book):

- Logging and log management (Requirement 10)
- Encryption of stored data (Requirement 3.4)
- Application security in case of internal applications (Requirement 6.5)

The key point to remember is that the compensating controls should be better or more secure than the original requirement and not simply be a poor substitute. Despite this strict definition, the QSAs in the field often have to deal with unsuitable and ineffective compensating control suggestions from the merchants.

Overall, PCI DSS allows organizations to make progress towards security of the card data. Despite that progress, some of the PCI controls are often missing from breached environments. For example, Verizon PCI Report 2010 shows:

Table 1. Assessment findings at IROC by PCI DSS Requirement.

PCI DSS Requirement	% of Organizations*
1: Install and maintain a firewall configuration to protect data	46%
2: Do not use vendor-supplied defaults for system passwords and other security parameters	48%
3: Protect stored data	43%
4: Encrypt transmission of cardholder data and sensitive information across public networks	63%
5: Use and regularly update anti-virus software	70%
6: Develop and maintain secure systems and applications	48%
7: Restrict access to data by business need-to-know	69%
8: Assign a unique ID to each person with computer access	44%
9: Restrict physical access to cardholder data	59%
10: Track and monitor all access to network resources and cardholder data	39%
11: Regularly test security systems and processes	38%
12: Maintain a policy that addresses information security	44%

(Source: Verizon Business PCI Report 2010)

These control areas marked in red present the most difficulties to most organizations. On top of this, legacy systems such as older mainframe and midrange systems often lack controls of modern systems but house massive amounts of regulated data. Implementing these and other controls on such systems often takes more resources than the rest of the cardholder data environment.

Most Challenging PCI Controls – Ongoing Monitoring

According to the Verizon PCI report, the logging and monitoring (Requirement 10), regular testing (Requirement 11) and encryption of stored data (Requirement 3) are the hardest to comply with and most often missing from organizations worldwide.

What most of the above controls have in common are ongoing requirements! The controls that call for ongoing, daily effort are harder. Monitoring access to card data must be continuous to be effective against data breaches. The log review, the key part of Requirement 10.6, is explicitly mandated to occur on a daily basis.

PCI DSS prescribes the following types of monitoring and ongoing review:

- Log review (Requirement 10.6)
- IDS/IPS monitoring (Requirement 11.4)
- Monitoring for critical file changes (Requirement 11.5)
- Monitor vendor remote access (Requirement 8.5.6)

Also, as a matter of process, the merchant must monitor their environment for missing technical PCI DSS controls – password policy, anti-virus tools, firewall configurations, etc.

But it is not enough to monitor! The merchant also needs to prove that such ongoing monitoring is in place. These and other PCI DSS activities are proven to assessors during the annual assessment by showing the evidence. Such PCI compliance evidence might include reports, incident log records or even screen capture videos and other collected activity metadata. In some cases, even the presence of an advanced monitoring tool and clear evidence of its operational status was enough to demonstrate PCI diligence to a QSA.

Technical controls are often evidenced by actual configuration files (technology proof), screen captures, logs and other IT data. Policy controls are evidenced by documented practices (and evidence of following them).

Let's consider a few real-world scenarios where the monitoring challenges discussed above come to an extreme. These are:

- Cloud or outsourced applications
- Outdated legacy applications, possible deployed on an outdated system
- Custom applications written in a non-compliant manner

Let’s review these scenarios in detail and look at the options at solving them.

Cloud Application Scenario

For cloud applications that are accessed by IT users from their desktops, monitoring at the cloud end might not be possible in many cases due to provider policies and practices. In any case, not all local user activities would be visible at the remote end. On top of this, getting logs and other monitoring data from a cloud provider might not have the granularity needed for PCI DSS.

On the other side, if a browser is used to access the application (the most common route), the local logging will not be adequate either. As a result, a company will have an application that touches sensitive and regulated data which would not be able to be monitored and won't have PCI-mandated logs to review.

For example, a common scenario includes using a cloud CRM such as Salesforce.com or Netsuite. A web browser is used to connect to the application and perform actions with data at the cloud end. Limited logs are available from a service provider. No local logging for user actions will be present. PCI DSS still mandates that logs be created and reviewed, but none are present by default.

Monitoring in such an environment calls for a new, creative approach.

Custom Application Scenario

Custom applications, scripts, including modified and open source payment applications, are still a reality at many merchants. In addition, stored credit card data, accumulated at branch offices and corporate data centers, is commonly accessed for various analytics purposes by other applications. These analytic applications, used by marketing departments, are often not written based on PCI-mandated security procedures. Many smaller merchants also chose to use open-source and freeware applications with regulated data.

For example, an open source CRM or a shopping cart application may be modified by the merchant over the course of many years. Logging – at the levels prescribed by PCI DSS – is not likely to be present, especially if the original application had a code base developed many years ago. What's worse, some of such applications predate PCI DSS security standards.

Monitoring these applications requires a different method, rather than rewriting the application to include logging.

Legacy Application Scenario

While mobile devices and Windows 7 desktops are a common sight across the IT landscape worldwide, many store environment as well as hotels, restaurants and even financial companies still use legacy platforms and legacy applications for sensitive and regulated data processing. Over the years, these platforms, such as mainframes and mid-range systems, older servers and even Point-of-Sale (POS) terminals have been entrenched and are likely to be removed when they break down. Establishing PCI DSS compliance and implementing PCI controls, including security monitoring and log review, in such an environment presents a unique challenge since many of these systems simply do not have PCI-prescribed security capabilities. Despite that, they still need to be monitored and secured – since PCI has no "grandfathering" clause. Customized legacy applications are even more costly to replace as engineers who made the changes might have retired years ago. Modern systems, such as

desktops and mobile devices, interface with such ancient systems via middleware and connectors, which creates additional risks and additional monitoring problems. In such environments, the only way to monitor is by using a dedicated security application to record user actions and effectively create PCI-quality audit trails, which tie the users and their actions together in a clear and unambiguous way.

Monitoring legacy platforms and applications requires actually *creating* all the audit information by the monitoring application that watches for user operations with regulated data.

Debugging Logs Only Scenario

Another common case is when an application in scope for PCI DSS does have logging, but such logging falls far short of compliance requirements. Inadequate logging is common in legacy applications. Another common scenario is applications where logging was designed purely for operational and debugging purposes and not for security and compliance audits.

PCI DSS does present specific requirements for information that must appear in each log entry:

PCI DSS Requirements
10.3.1 User identification
10.3.2 Type of event
10.3.3 Date and time
10.3.4 Success or failure indication
10.3.5 Origination of event
10.3.6 Identity or name of affected data, system component, or resource.

(Source: PCI DSS v2.0 from PCI Council website)

The best example of such logging is using Windows Event Logs for tracking access to documents on a shared file server. A lot of log entries will be created if access logging is enabled, but it will be hard to determine compliance and security impact of such events – it is even hard to know whether the regulated file has been modified based on such inadequate logs.

PCI DSS and other regulations imply that logs are clear records of user and system activity that can be used by internal security personnel and auditors to determine "who did what" with regulated data. Such logs must be granular, clear, and readable by the reviewers

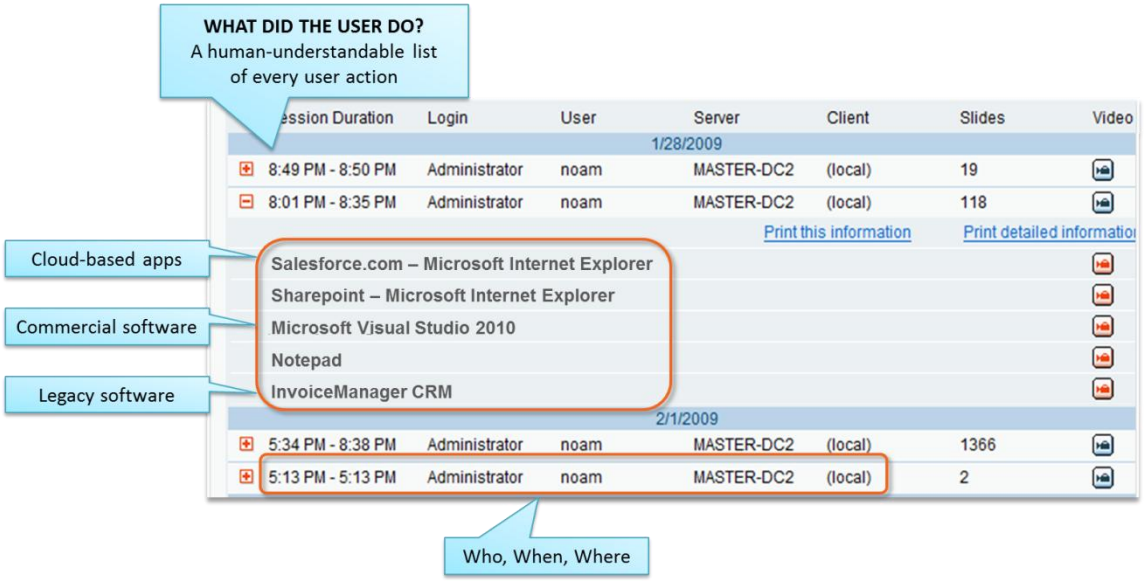
In such cases, it is often easier to actually *create* all the audit information by the monitoring application that watches for user operations with regulated data and not trust the built-in inadequate logging.

Solving the Worst Case Monitoring Problems

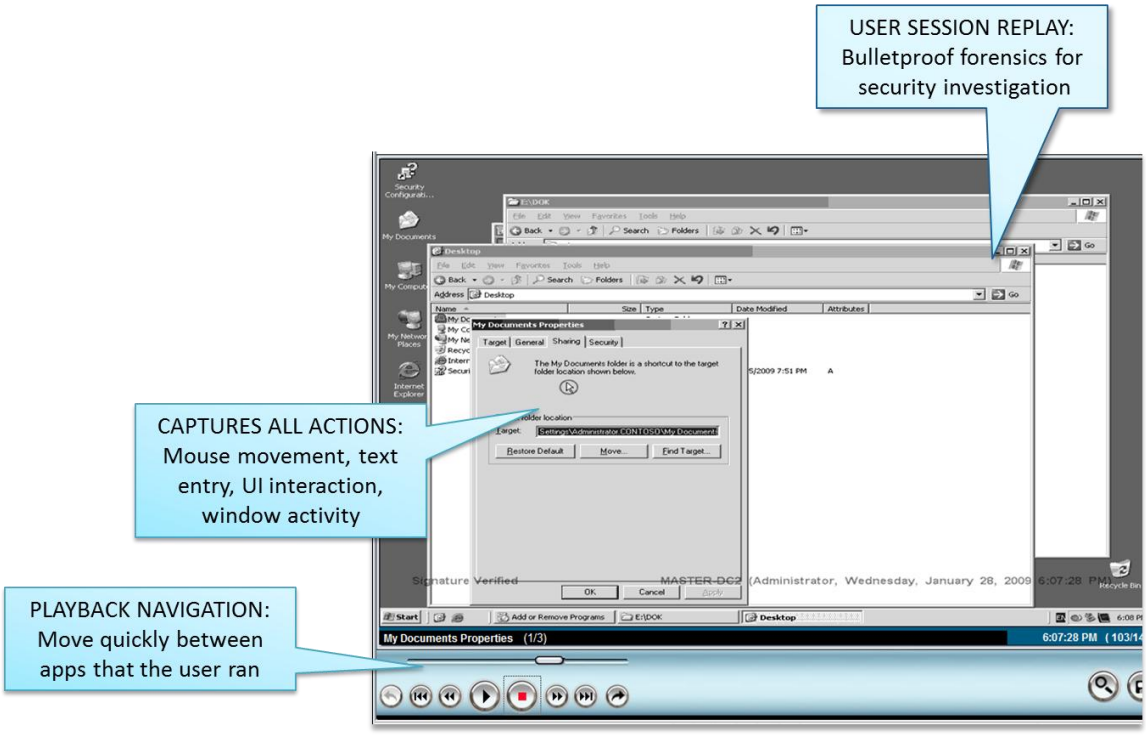
The right solution for "cracking the nut" of PCI DSS controls and security for environments where logging and monitoring are next to impossible is in "making your own logs" where none exist or "making better logs" where logs are inadequate for facing the challenges. Technologies such as ObserveIT make that possible. ObserveIT auditing software acts like a security camera on your servers, creating logs and enabling PCI DSS monitoring. It does the following:

- Make logs where none exist by recording text logs and video replay of every app (even apps with no internal logs!), over every session protocol (SSH, RDP, Citrix, VMware, etc.) on Windows, Unix and Linux
- Enable better logging and achieve accountability when shared-user logins (ex: 'administrator') are tied to specific named users
- Help you review and analyze the records by using compliance reports and build-your-own forensic searches that meet your compliance and security needs

Here is how ObserveIT shows the user activity data – effective for cloud, legacy and custom applications



The following view shows that ObserveIT can also record actions that are never logged, but are extremely useful for regulatory reviews as well as security monitoring. Log generation of every user action combined with exact screen-by-screen video recording of what took place allows for activity monitoring all around regulated data.



Overall ObserveIT has critical value for PCI compliance in the following domains:

- Provide external vendor access monitoring and gain insight exactly what 3rd party vendors are doing (PCI DSS requirement 8.5.6)
- Drastically simplify log review by creating “human readable logs” – and enhanced obscure system logs are by additional clear human-readable logs (Requirement 10.6)
- Tie each shared-user session recording to a specific named user (Requirement 10.1)
- Enable log creation where logs don't exist but monitoring is still mandatory: cloud application, legacy application and custom application with no own logging (Requirement 10)
- Simplify user policy monitoring (Requirement 12)

Finally, ObserveIT technology serves as a key compensating control for logging and monitoring in PCI DSS environment. Such solutions are indeed the only way to comply with Requirement 10 for the above scenarios. By being able to track every access to servers and databases, cloud applications, legacy and custom applications and, in essence, audit people and their actions and not just systems, ObserveIT follows the original spirit of PCI DSS. PCI DSS was created for protecting data from attacks and threat agents and your organization actions around PCI DSS should enable useful security monitoring and not simply record obscure system-level data.

Total PCI DSS control coverage by ObserveIT solutions can be found at the website.

Brief Case Study

A customer case study demonstrates the challenges and solutions discussed above. An ecommerce retailer Example.com uses hosted web servers, virtual datacenter, and cloud-based CRM application to run their business. In essence, most critical business systems are not managed by the internal IT personnel. However, this does not change how PCI DSS applies to this business: they still need to perform monitoring and track vendor access to their outsourced systems. In addition, they have to monitor how internal personnel touches stores of cardholder data (such as for refunds and ongoing purchase purposes).

Initially, the organization has attempted to harness all the logs available from individual systems and combine the logs obtained from their service provider partners and outsourcers. This approach has run into the wall because many of the logs were missing, not available for all data access methods, or clearly inadequate for compliance monitoring and investigation purposes. Logs simply did not paint a complete picture of card transaction activity across the entire stack of applications.

Instead, Exmple.com chose to implement ObserveIT to unify all monitoring using the agents deployed on all systems that either access or store cardholder data, including desktop to connect to cloud applications containing payment cards. This allowed them to create a unified audit trail useful for security monitoring and PCI assessment.

Conclusions and Action Items

The key points to remember is that regulatory mandates compel organizations to monitor their environment for security issues – even in the absence of a simple way of doing so. In case of PCI DSS, monitoring a challenging environment can be accomplished by using applications that create logs, metadata and even screen capture videos of regulated data operations. On top of this, such technology can be used to "bulk up" logging for situations where existing logs are not adequate for incident investigations, security monitoring as well as fall short of regulatory requirements.

The actions items are:

- Review how you monitor cloud, legacy and custom application that touch regulated data
- Deploy technology to create or enrich existing audit logs for improved, compliant monitoring
- Review your PCI DSS compensating control for application monitoring, vendor activity and logging to make sure they satisfy PCI guidelines

About the author

Dr. Anton Chuvakin (http://www.chuvakin.org) is a recognized security expert in the field of log management and PCI DSS compliance. Anton leads his security consulting practice www.securitywarriorconsulting.com, focusing on logging, SIEM, security strategy and PCI DSS compliance for security vendors and Fortune 500 organizations.

He is an author of books "Security Warrior" and "PCI Compliance" and a contributor to "Know Your Enemy II", "Information Security Management Handbook"; he is now working on a book about computer logs. Anton has published dozens of papers on log management, correlation, data analysis, PCI DSS, security management (see list www.info-secure.org) . His blog http://www.securitywarrior.org is one of the most popular in the industry.

In addition, Anton teaches classes (including his own SANS class on log management) and presents at many security conferences across the world; he recently addressed audiences in United States, UK, Singapore, Spain, Russia and other countries. He works on emerging security standards and serves on the advisory boards of several security start-ups.

Dr. Anton Chuvakin was formerly a Director of PCI Compliance Solutions at Qualys. Previously, Anton worked at LogLogic as a Chief Logging Evangelist. Before LogLogic, Anton was employed by a security vendor in a strategic product management role. Anton earned his Ph.D. degree from Stony Brook University.